2015

Iterative phase retrieval algorithms. I: Optimization

Changliang Guo
University College Dublin

Shi Liu
Washington University School of Medicine in St. Louis

John T. Sheridan
University College Dublin

applied optics

Iterative phase retrieval algorithms. I: optimization

CHANGLIANG GUO,[1] SHI LIU,[2] AND JOHN T. SHERIDAN[1,*]

[1]School of Electrical, Electronic and Communication Engineering, Communications and Optoelectronic Research Centre, The SFI-Strategic Research Cluster in Solar Energy Conversion, College of Engineering and Architecture, University College Dublin, Belfield, Dublin 4, Ireland
[2]Department of Radiation Oncology, School of Medicine, Washington University in St. Louis, Missouri 63110, USA
*Corresponding author: john.sheridan@ucd.ie

Received 19 January 2015; revised 24 March 2015; accepted 26 April 2015; posted 27 April 2015 (Doc. ID 232602); published 14 May 2015

Two modified Gerchberg–Saxton (GS) iterative phase retrieval algorithms are proposed. The first we refer to as the spatial phase perturbation GS algorithm (SPP GSA). The second is a combined GS hybrid input–output algorithm (GS/HIOA). In this paper (Part I), it is demonstrated that the SPP GS and GS/HIO algorithms are both much better at avoiding stagnation during phase retrieval, allowing them to successfully locate superior solutions compared with either the GS or the HIO algorithms. The performances of the SPP GS and GS/HIO algorithms are also compared. Then, the error reduction (ER) algorithm is combined with the HIO algorithm (ER/HIOA) to retrieve the input object image and the phase, given only some knowledge of its extent and the amplitude in the Fourier domain. In Part II, the algorithms developed here are applied to carry out known plaintext and ciphertext attacks on amplitude encoding and phase encoding double random phase encryption systems. Significantly, ER/HIOA is then used to carry out a ciphertext-only attack on AE DRPE systems.

OCIS codes: (060.4785) Optical security and encryption; (060.4510) Optical communications; (110.2960) Image analysis; (100.0100) Image processing; (100.5070) Phase retrieval.

http://dx.doi.org/10.1364/AO.54.004698

1. INTRODUCTION

Phase retrieval problems arise in a number of areas, such as astronomy, electron microscopy, wavefront sensing, holographic imaging, coherence theory, and when tracking inverse-scatter problems [1–16]. The classical method to iteratively recover the phase from two intensity measurements (images) was proposed by Gechberg and Saxton in 1972 and is referred to as the GS algorithm (GSA) [1]. In 1978, in order to reconstruct an object distribution from the modulus of its Fourier transform (FT), Fienup proposed two modified GSAs: the error reduction (ER) algorithm (ERA) and the hybrid input–output (HIO) algorithm (HIOA) [2]. The HIOA improves on the ERA and has been extremely popular when performing phase retrieval. It has been widely applied in reconstructing the object field given the modulus of its FT [2–19]. Despite the usefulness of these techniques, care must be taken when applying them.

When using GSA or HIOA (or any of the algorithms proposed in this paper), we note that, if the input signal is not of finite extent (i.e., space limited) or the sampling in the Fourier domain is not fine enough, i.e., at the Nyquist sampling rate, the phase in the object domain and in the Fourier domain will not be successfully retrieved because of aliasing [3,20]. Care must also be taken when applying iterative techniques, as they can sometimes stagnate before converging to an acceptable solution and/or exhibit a relatively slow convergence rate [21]. This issue will be later discussed in greater detail.

In this paper, a modified version of the HIOA proposed by Fienup [2] is used, as amplitude information in the input and Fourier domains are explored for phase retrieval. Then, a combined GS and the modified HIO algorithm (GS/HIOA) and a new spatial phase perturbation GS algorithm (SPP GSA) are introduced in an attempt to ensure that the iteration process avoids converging to a local minima of the cost function (CF) and, thus, can achieve better and faster convergence. Applying these algorithms is shown to increase the likelihood of success in retrieving the phase in the space and the Fourier domains. Thus, a comparison between the GS/HIO and SPP GS algorithms is presented.

In some phase retrieval problems, the input field is unavailable. To retrieve the phase given only the amplitude of the Fourier image, other constraints are necessary. In this paper, the shape of the object, which is also called support of the object, is used to provide the additional constraints. The shape is the area in the object image outside of which the pixel values are all zero. The support can be obtained from the autocorrelation

of the object. This is discussed in detail. Then, in this case, the ERA is combined with the classical HIOA (ER/HIOA) to perform successful phase retrieval. A comparison between the performance of the HIO and ER/HIO algorithms is also performed.

Phase retrieval algorithms have recently been applied as part of attacking methods to test the vulnerability of the classical amplitude encoding (AE) FT-based double random phase encryption (AE DRPE) system, to a known plaintext ciphertext attack (KPCA) [22]. In Part II, the algorithms developed here are used to carry out KPCAs on amplitude encoding (AE) and phase encoding (PE) DRPE systems. Cryptanalysis in the case of ciphertext only attacks (COA) is also discussed. It is demonstrated that applying the ER/HIOA successful COAs on AE DRPE systems can be carried out with much better results than previously reported [23].

Part I is structured as follows: In Section 2, we first review the GS and HIO algorithms separately and show how they can be usefully combined. The combined ER and HIO algorithm is presented. Then, the new SPP GS algorithm is described. In Section 3, the results of our comparison between the performances of the GS, HIO, GS/HIO, and SPP GS algorithms are presented. Then, the performance of the ER/HIOA in retrieving the signal phase given only the signal's amplitude in the Fourier domain is presented, as is a method to determine tighter limits (precise conditions) on the support (extent) of the object in the input domain. A brief conclusion is given in Section 4.

In Part II, the algorithms developed here are applied to perform KPCAs on both AE- and PE-based DRPE systems, and successful COAs are carried out on AE DRPE systems [24].

2. THEORETICAL ANALYSIS: GSA, HIOA, AND SPP GSA

A. GSA-Based Phase Retrieval

The Gerchberg–Saxton algorithm (GSA) [1] was originally proposed in connection with the problem of reconstructing phase information given only amplitude information in the space and Fourier domains, i.e., given two intensity measurements, one in the input domain and the other in the spatial frequency (FT) domain, i.e., the signals power spectral distribution (PSD). The GSA has been successfully applied to recover phase from intensity measurements in astronomy, x-ray crystallography, electron microscopy, and in wavefront sensing [1].

A flow chart illustrating the retrieval of phase from two such intensity measurements using the GSA is shown in Fig. 1 [1]. First, an initial guess of the signal phase in the Fourier domain is made, i.e., $\varphi_1(u,v)$. The initial phase values assigned to each pixel location are typically uniformly distributed between $-\pi$ and π, produced using a random number generator. Then, the resulting 2D phase signal, $e^{i\varphi_1(u,v)}$, is multiplied by the real valued amplitude $|F(u,v)|$ calculated by taking the square root of the measured intensity in the Fourier domain. An inverse Fourier transform is performed. Then, in the object domain, while the resulting phase distribution is retained, the calculated amplitude is replaced by the input amplitude in the spatial domain $|f(x,y)|$. The resulting distribution is then Fourier transformed back to the Fourier domain, and the phase is once

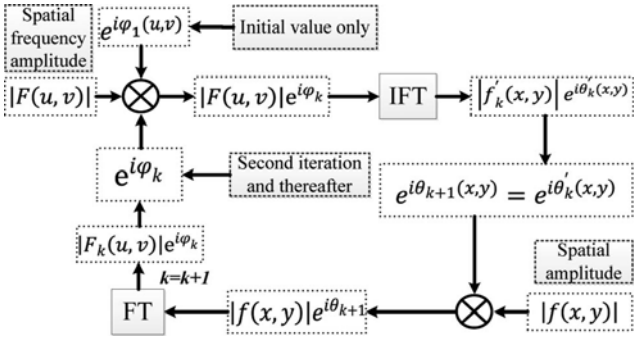

Fig. 1. Flow chart of the standard GSA for iterative retrieval.

again retained for the next iteration. The iterative process continues until a cost function, e.g., the sum squared error (SSE) (which is discussed later), drops below some threshold value chosen to indicate that acceptable convergence has been achieved.

Following Fig. 1, the kth iteration of GSA can be mathematically expressed as

$$F'_k(u,v) = |F(u,v)|e^{i\varphi_k(u,v)}, \tag{1a}$$

$$f'_k(x,y) = |f'_k(x,y)|e^{i\theta'_k(x,y)} = \mathcal{F}^{-1}\{F'_k(u,v)\}, \tag{1b}$$

$$f_{k+1}(x,y) = |f(x,y)|e^{i\theta_{k+1}(x,y)} = |f(x,y)|e^{i\theta'_k(x,y)}, \tag{1c}$$

$$F_{k+1}(u,v) = |F_{k+1}(u,v)|e^{i\varphi_{k+1}(u,v)} = \mathcal{F}\{f_{k+1}(x,y)\}. \tag{1d}$$

The phase retrieval problem is equivalent to retrieving complex $f(x,y)$ if its magnitude and autocorrelation are known, i.e., given $|F(u,v)|^2$ [20]. The GSA works well when both the input complex image is space-limited and band-limited; therefore, the signal information in the Fourier domain is unambiguously preserved since the signal has been appropriately sampled to avoid aliasing. However, as will be demonstrated, if the complex-valued input plane signal is space-limited only, the GSA almost always stagnates and fails to converge, below an acceptable threshold, to a solution. In such cases, the phases in the input image spatial domain and in the Fourier domain are not satisfactorily retrieved.

B. HIOA, ER/HIOA, and GS/HIOA

1. HIOA

In [2], Fienup proposed the HIOA in order to speed up convergence of the error reduction algorithm (ERA) (discussed later in greater detail). This approach solves the phase retrieval problem in which the object image is retrieved given the amplitude in the Fourier domain and a set of constraints. At the kth iteration, $f_k(x,y)$, the estimate of the object image, is Fourier transformed. In the Fourier domain, the amplitude is forced to have the known modulus values while the phase is retained. The result is then inverse transformed, giving the kth approximation to the image $f'_k(x,y)$. The iteration only continues after the new estimate of the object is forced to

conform to the known object domain constraints. In the classical HIO algorithm, the $(k+1)$th iteration is presented by [19]

$$f_{k+1}(x,y) = \begin{cases} f'_k(x,y), & \text{otherwise} \\ f_k(x,y) - \beta f'_k(x,y), & (x,y) \in \gamma' \end{cases} \quad (2)$$

where γ includes all points at which $f'_k(x,y)$ violates the required constraints. The factor β is a constant feedback parameter, with values residing between 0.5 and 1, has been found to produce good results [25].

In this paper, we apply the HIOA with slight modifications to solve the two-measurement phase retrieval problem, i.e., retrieving the phase in the object plane given the amplitudes in the object and the Fourier domains. The HIOA is identical to the GSA during the steps shown in Eqs. (1a), (1b), and (1d). However, the calculation of the third step is replaced by

$$f_{k+1}(x,y) = \begin{cases} |f(x,y)|e^{i\theta'_k(x,y)}, & \text{otherwise} \\ f_k(x,y) - \beta f'_k(x,y), & (x,y) \in \gamma' \end{cases} \quad (3)$$

where the parameter γ indicates the region where the pixel values are 0 in the object image $|f(x,y)|$. This region can, in general, be easily identified for a given object image. Concerning the two-measurement phase retrieval problem, it will be shown that the HIOA works better than the GSA. The phases in the space and Fourier domains can be retrieved with some noise, but, as will be shown, the HIOA still does not, in general, converge to the global minimum.

2. Error-Reduction Algorithm and ER/HIOA

In [2], the author also introduced a modified version of the GSA, which is referred to as the error-reduction algorithm (ERA). The ERA differs from the HIOA [see Eq. (2)], in that the $(k+1)$th iteration of the ERA is presented by [2]

$$f_{k+1}(x,y) = \begin{cases} f'_k(x,y), & \text{otherwise} \\ 0, & (x,y) \in \gamma' \end{cases} \quad (4)$$

where once again γ includes all points at which the kth approximation of the object image $f'_k(x,y)$ violates the object extent constraints.

In this paper, in order to improve convergence, the ER and HIO algorithms are combined, giving what we refer to as the ER/HIO algorithm. The ER/HIOA operates as follows: during the phase retrieval process, ERA is first performed with a number of iterations followed by the classical HIOA, i.e., Eq. (2), which is performed with several iterations. This combination (cycle) is then repeated as necessary. The ER/HIOA has been found to work better than using either the ERA or HIOA alone, and, as will be shown, results in a more accurate object and phase information being retrieved [17,19,20,25–28]. The operation of the ER/HIOA is illustrated in Fig. 2.

The K parameter appearing in Fig. 2 is the maximum number of iterations the ER/HIOA is performed. k indicates the kth iteration. K_p is the number of iterations in each cycle of ER/HIOA [25]. K_1 is the number of iterations the ERA is performed; therefore, $K_p - K_1$ is the number of iterations of the HIOA performed in each cycle. When using the ER/HIOA, we indicate this using the notation $(K_1, K_p - K_1)$. N and Y shown in Fig. 2 indicate *No* and *Yes*, respectively.

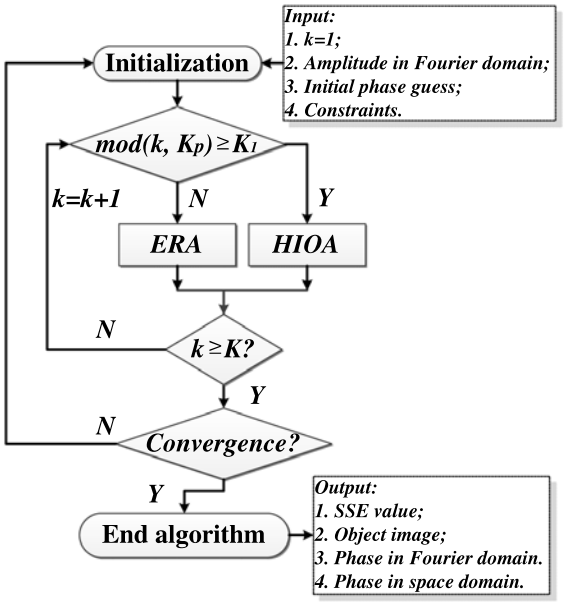

Fig. 2. Illustration of the process of performing the ER/HIOA $(K_1, K_p - K_1)$.

3. GS/HIOA: Two-Measurement Phase Retrieval

Similarly, we also propose a combined GS and HIO, following Eq. (3), algorithm, which we refer to as the (GS/HIOA). The GS/HIOA requires that, during the phase retrieval process, we cyclically perform several iterations of GSA followed by several iterations of HIOA, according to Eq. (3). The flow chart of the process is shown in Fig. 3.

As in the ER/HIOA, K is the maximum number of iterations the GS/HIOA is performed, k is kth iteration, K_p is the number of iterations in each cycle of GS/HIOA, K_1 is the number of iterations of the GSA performed, and $K_p - K_1$ indicates the number of iterations of the HIOA performed in each cycle. We indicate this by GS/HIOA $(K_1, K_p - K_1)$.

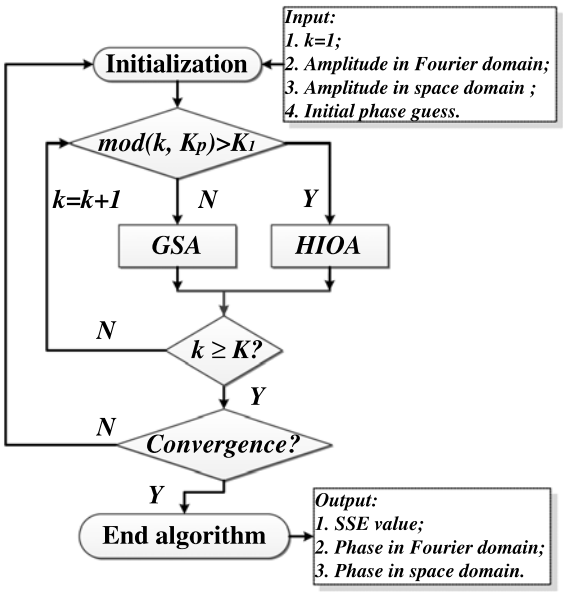

Fig. 3. Illustrated process of performing GS/HIOA $(K_1, K_p - K_1)$.

C. SPP GS Phase Retrieval Algorithm

As noted, one of the difficulties encountered in using the GSA is its tendency to converge to incorrect solutions. In order to ensure that the GSA does not become stuck in local minima, we propose to add a small random perturbation into the phase found in the space plane during each iteration. The approach is somewhat reminiscent of the simulated annealing approach [29], as the amount of noise added decreases with each iteration. The algorithm involves the following steps:

Step 1: Generate an initial spatial phase $e^{i\varphi_1(u,v)}$ using a random number generator, i.e., each pixel value of $\varphi_1(u, v)$ is normally distributed between $[-\pi, \pi]$; this is multiplied by the amplitude of the Fourier image field $|F(u, v)|$.
Step 2: The resultant complex image of Step 1 is inverse Fourier transformed to give a distribution in the object domain.
Step 3: A perturbation in the spatial phase $\Delta\theta_k(x, y)$, the size of which is chosen to decrease linearly with the number of iterations performed, is added to the phase output from Step 2, and the resultant modified phase screen values are multiplied by the object image $|f(x, y)|$.
Step 4: The complex image field produced in Step 3 is then Fourier transformed back to the Fourier domain.
Step 5: The phase is preserved and multiplied by the known amplitude of the Fourier plane field $|F(u, v)|$ for use as the input in the next iteration.

The iteration process is then repeated until the algorithm converges to a satisfactory solution.

The equations governing the algorithm during the kth iteration are

$$F_k(u, v) = |F_k(u, v)|e^{i\varphi_k(x,y)} = \mathcal{F}\{f_k(x, y)\}, \tag{5a}$$

$$F'_k(u, v) = |F(u, v)|e^{i\varphi_k(u,v)}, \tag{5b}$$

$$f'_k(x, y) = |f'_k(x, y)|e^{i\theta'_k(x,y)} = \mathcal{F}^{-1}\{F'_k(u, v)\}, \tag{5c}$$

$$f_{k+1}(x, y) = |f(x, y)|e^{i\theta_{k+1}(x,y)} = |f(x, y)|e^{i[\theta'_k(x,y)+\Delta\theta_k(x,y)]}. \tag{5d}$$

The additional perturbation of the phase $\Delta\theta_k(x, y)$ is defined as follows:

$$\Delta\theta_k(x, y) = \alpha \times \{\text{rand}_{(-1,1)}(x, y)\}_k \times \left(1 - \frac{k'}{K'}\right),$$
$$\text{where } 0 < K' \le K, \quad \text{and} k' = \begin{cases} k, & 0 < k \le K' \\ K', & K' < k \le K \end{cases}. \tag{6}$$

α is scaling factor that determines the initial size of the perturbation and is set to $\pi/2$ in all the simulations results presented below. The value of the scaling factor was determined, based on observation of the performance of the algorithm. We note that it is important not to choose an initial value of α that is too small. This ensures that the perturbation introduced allows the algorithm to avoid convergence to a local minimum. $\{\text{rand}_{(-1,1)}(x, y)\}_k$ is a matrix generated at the kth iteration having the same dimensions as the zero-padded encrypted images being processed. Each value generated lies between −1 and 1. k indicates the kth iteration $(0 \le k \le K)$. K is the maximum number of iterations, while K' is the iterations, after which perturbations are no longer added to the spatial phase distribution. As indicated in Eq. (6), the perturbation size decreases linearly with the number of iterations, and, when $k \ge K'$, all the values in the $\Delta\theta_k(x, y)$ array equal 0, thus terminating the perturbation of the phase. A flow chart illustrating the algorithm is given in Fig. 4.

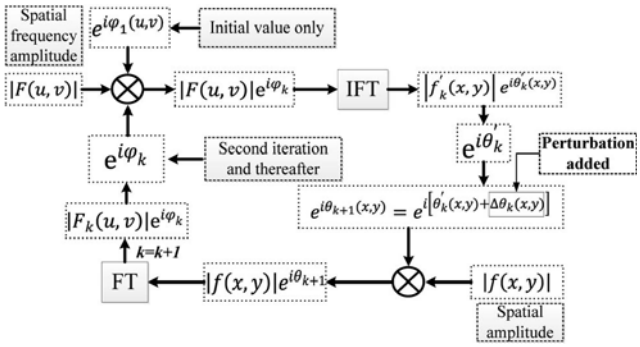

Fig. 4. Flow chart of the SPP GSA for iterative phase retrieval.

3. NUMERICAL SIMULATION: PHASE RETRIEVAL

A. Comparison of Different Phase Retrieval Algorithms

In this section, we compare the performance of the four phase retrieval algorithms: GS, HIO, GS/HIO, and SPP GS. The algorithms are all applied under identical conditions, i.e., using the same complex input image and the same initial phase value in the Fourier domain at the start of the phase retrieval iterative process. Our numerical simulation are performed in order to retrieve a random phase $e^{i\theta}$ applied to a known "Lena" image $|f(x, y)|$ and a given amplitude $|\mathcal{F}\{|f(x, y)|e^{i\theta}\}|$. We define the discrete sum squared error (SSE) used in all the numerical simulation results presented to be

$$\text{SSE} = 10\log_{10}\left\{\frac{\sum_{m=1}^{M}\sum_{n=1}^{N}\{|F_k(m, n)| - |F(m, n)|\}^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}\{|F(m, n)|\}^2}\right\}. \tag{7}$$

This cost function is employed to examine the convergence of all four algorithms.

In all the simulations, the Lena image of the size 128 × 128 is used as the input with an unknown superimposed spatial phase given by $e^{i\theta(m,n)}$, $m, n \in [1, 128]$, where each value of $\theta(m, n)$ is randomly distributed between $-\pi$ and π. As indicated in Fig. 5, both the Lena image and the phase screen information are zero padded to 256 × 256 in order to avoid aliasing effects. Increasing the input image area by a factor of four by zero padding is equivalent to doubling the sampling rate in both dimensions [11]. $|\mathcal{F}\{|f(x, y)|e^{i\theta}\}|$ is shown in Fig. 5(c).

In Fig. 6, the values of SSE are plotted as functions of the number of iterations k. As noted, the parameter β in Eq. (3) is set equal to 1/2. When using the GS/HIOA, if a single iteration

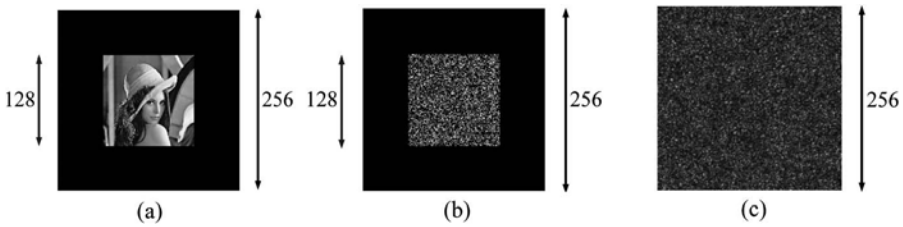

Fig. 5. (a) Lena image $|f(x,y)|$. (b) Phase values $\theta(-\pi \le \theta \le \pi)$ at the input plane. (c) Amplitude $|\mathcal{F}\{|f(x,y)|e^{i\theta}\}|$.

is first performed using the GSA followed by 99 iterations using HIOA, then 100 iterations constitute one cycle, and we indicate this by (1, 99). In total, 10 such cycles are performed. We can see from Fig. 6 that, after 100 iterations, the SSE values in the GSA and HIOA cases (blued dashed curve and dotted black curve, respectively) stagnate at values of around −8 to −12 dB, respectively, and no further improvement is observed for larger numbers of iterations. However, applying the GS/HIOA (red solid curve) with (1, 99), it can be seen that, after only 101 iterations, the SSE value drops rapidly to −60 dB. Then, following $k = 201$ iterations, another significant drop occurs, which happens again when $k = 301$. Finally, when $k > 401$ iterations, the value decreases to −300 dB, and no further improvement is observed. The sudden decreases taking place at 101, 201, and 301 iterations indicate that the drops occur when the GSA is reapplied (recall that each cycle of 100 iterations equals 1 GSA iteration followed by 99 HIOA iterations).

Several questions arise. For example, would the observed decrease happen faster if a shorter cycle were used? To explore this in Fig. 7, the GS/HIOA is applied, and we compare the SSE values for different iteration cycles (from 20 to 100 iterations) with the GSA being performed just once at the beginning of every cycle. In each case, we run the GS/HIOA process 10 times using different initial phase guesses in the Fourier domain to start the iteration. The resulting average SSE values are plotted. Examining Fig. 7, the (c) curve (colored red), which corresponds to the case of 1 GS iteration followed by 39 iterations HIOA in each cycle, i.e., (1, 39) (red curve), converges to −300 dB in less than 500 iterations (12 cycles). Therefore, this cycle produces the best result for the cases examined. However, we note, based on the results presented in Fig. 7, that the cycles (1, 29) and (1, 49) also perform satisfactorily compared to (1, 39) and also retrieve the global minimum.

A second question that arises is what is the effect of increasing the number of GSA iterations in each cycle? Having identified the GS/HIOA (1, 39) as being in some sense optimized, the number of iterations of GSA k_1 performed was increasing to 10, 20, and 30, assuming a cycle of 40. No significant improvement was observed and, in general, inclusion of just one iteration of the GSA per cycle was found to be sufficient in order to ensure rapid convergence.

Now we wish to compare the performances of the SPP GS, GS, and HIO algorithms under identical conditions. The results are shown in Fig. 8. In the simulation, we set $K = 10000$ and $K' = K/2$ [see Eq. (6)]. As can be seen in Fig. 8, after 2000 iterations, the SSE in the SPP GSA case (purple curve) starts to drop dramatically, reaching −300 dB after 5000 iterations, indicating a distinct advantage compared with the GSA and HIOA. Furthermore the SPP GSA also converges slowly compared with the results found using the optimized GS/HIOA (1, 39), which reaches −300 dB after just 500 iterations. The SPP GSA appears to be effective because the perturbation of the phase reduces the possibility of the retrieved phase becoming stuck in local minima. In this sense, the proposed algorithm appears similar in its approach to the simulated annealing algorithm.

Several other tests were performed with the algorithms being applied for a wide range of cases, e.g., initial random phases φ_1, and it was found that the SPP GSA did not always converge. The SPP GSA's performance has been found to depend critically on the value of the initial random phase guess used in the Fourier domain as well as on the value of K'. In general, several

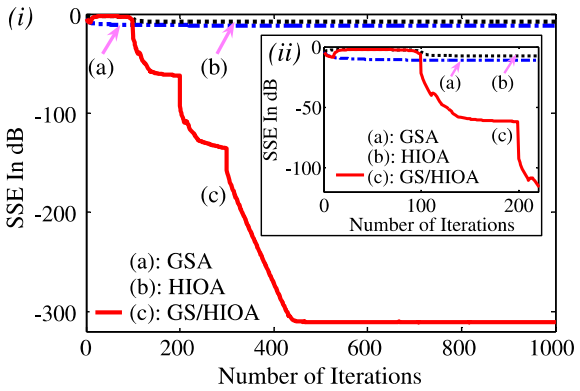

Fig. 6. SSE values using the GS, HIO, and GS/HIO (1, 99) algorithms. (i) $1 \le k \le 1000$. (ii) $1 \le k \le 220$.

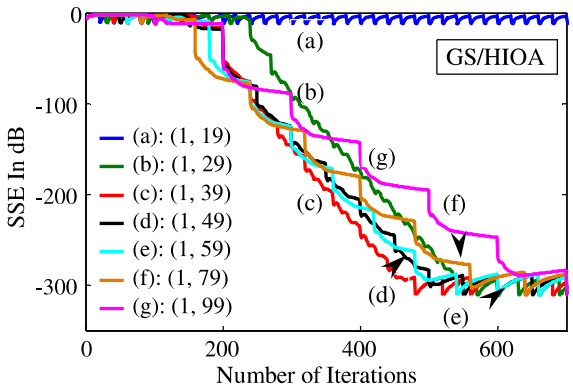

Fig. 7. SSE values using GS/HIOA with different cycles from (a) $K_p = 20$ to (g) $K_p = 100$, respectively.

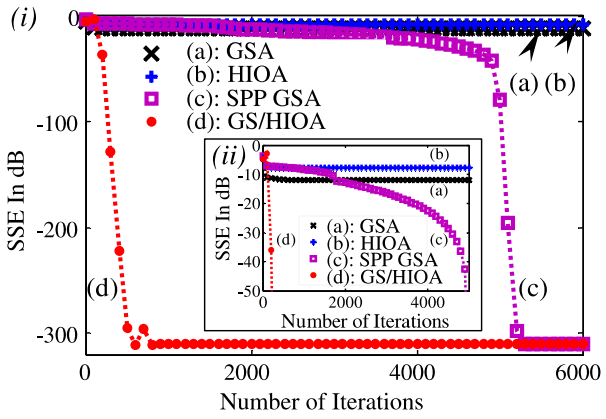

Fig. 8. SSE as a function of the number of iterations for the GS, HIO, SPP GS, and GS/HIO (1, 39) algorithms. (i) $1 \le k \le 6000$. (ii) $1 \le k \le 5000$.

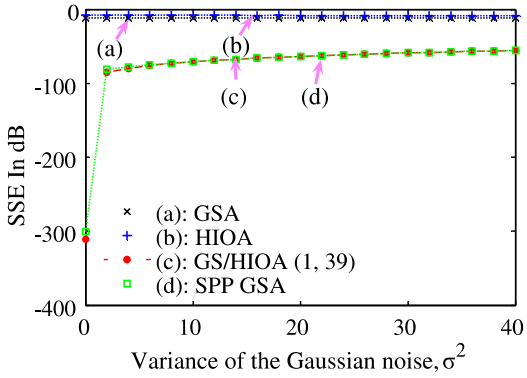

Fig. 10. SSE after 6000 iterations as a function of the variance of Gaussian noise, σ^2, added to the GS, HIO, SPP GS, and GS/HIO (1, 39) algorithms.

attempts using different initial guesses were necessary to ensure successful convergence. However, compared with either the GS or HIO algorithms alone, the SPP GSA works well and can reach the global minimum. This indicates that, despite its limitations, it can, if appropriately used, be employed to successfully solve the phase retrieval problem.

We denote the retrieved phase obtained in the Fourier domain at the kth iteration by φ'_k, while the true phase is denoted by φ In order to test the validity of the algorithms, a comparison is performed between the retrieved and the true phases. We define the phase error to be $\Delta\varphi = \mathrm{mod}(\varphi - \varphi'_k, 2\pi)$. $\Delta\varphi$ is obtained using the in-built MATLAB function "mod(-)" [30]. The errors present when using the different algorithms are shown in Fig. 9. As can be seen from Figs. 9(c) and 9(d), the differences between the retrieved phase and the true phase obtained when using the SPP GSA ($\Delta\varphi \approx 1$ rd) and GS/HIOA (1, 39) ($\Delta\varphi \approx 0.5$ rd) are almost constant values. We note that, although the SSE values for the HIOA, shown in Fig. 8(b), are higher than those for the GSA [see Fig. 8(a)], the retrieved phase difference ($\Delta\varphi \approx 0.25$ rd) obtained using the HIOA shown, i.e., Fig. 9(b), is a constant value with some slight noises added. Meanwhile the GSA produces a noise-like phase difference [see Fig. 9(a)], indicating the failure of the GSA. Therefore, although the HIOA SSE value is higher than that of the GSA, the HIOA iteration process is, in fact, correctly approaching the global minimum. Based on these results, it appears that examinations of the SSE values and the phase difference values are necessary when, as here, comparing the performances of different phase retrieval algorithms. The constant value of the phase errors is acceptable (and indicates successful retrieval) because any complex input object field containing additional constant phase errors will have the same amplitude in the Fourier domain.

We note that different constant values of the phase errors are obtained each time different initial phase guesses are used at the start of each algorithm. The values of the phase difference shown in Fig. 9, obtained using different algorithms

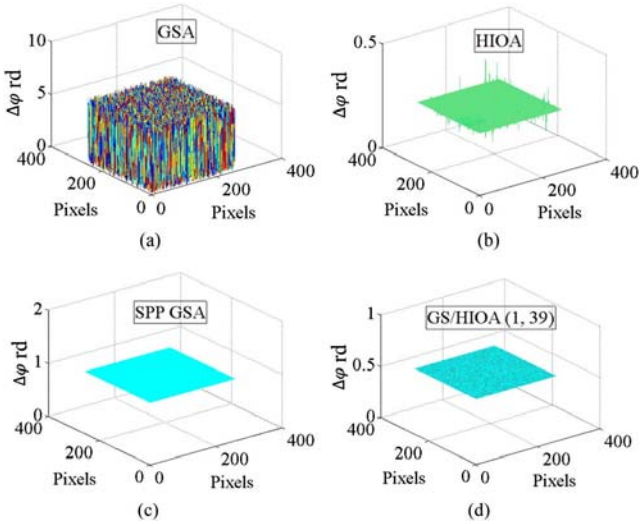

Fig. 9. $\Delta\varphi$ retrieved following 6000 iterations using (a) GS, (b) HIO, (c) SPP GS ($K' = 5000$), and (d) GS/HIO (1, 39) algorithms.

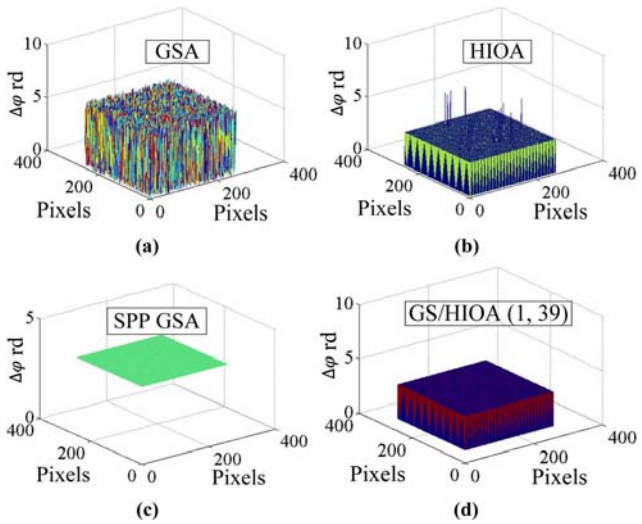

Fig. 11. $\Delta\varphi$ retrieved following 6000 iterations (with $\sigma^2 = 40$) using the (a) GS, (b) HIO, (c) SPP GS ($K' = 6000$), and (d) GS/HIO (1, 39) algorithms.

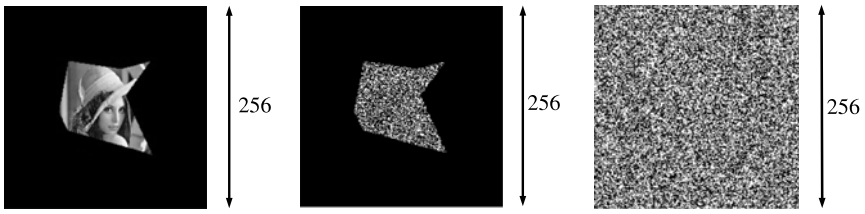

Fig. 12. (a) Unusually shaped Lena image $|f(x,y)|$ (256 × 256). (b) Phase values $\theta(-\pi \le \theta \le \pi)$ at the input plane. (c) Amplitude $|\mathcal{F}\{|f(x,y)|e^{i\theta}\}|$.

($\Delta\varphi \approx 0.5$ rd for GS/HIOA, $\Delta\varphi \approx 1$ rd for SPP GSA and $\Delta\varphi \approx 0.25$ for HIOA), do not appear to provide any information regarding the performance of the three algorithms.

Gaussian noise of mean 0 and variance σ^2 is added to the amplitude of the Fourier domain image. Then, for each case of the four algorithms, 6000 iterations are performed using the same initial phase guess in the Fourier domain. As shown in Fig. 10, with increasing variance σ^2 from 0 to 40, the SSE values for GSA and HIOA stagnate at about −10 dB, respectively. Applying GS/HIOA (1, 39) and SPP GSA, the SSE values decrease drastically to −100 dB when $\sigma^2 = 2$. Then, the SSE values continue decreasing slowly as σ^2 increases. Clearly, the performances of the GS/HIO and SPP GS algorithms continue to be much better than those of the HIO and GS algorithms, even in the presence of such Gaussian noise.

Next, the differences between the retrieved phases and the true phases, when the variance $\sigma^2 = 40$, for all four algorithms are presented in Fig. 11. We note the phase difference for GS/HIOA (1, 39) shown in Fig. 11(d) results in two values: $\Delta\varphi \approx 1.118$ rd and $\Delta\varphi \approx 4.259$ rd. The retrieved phase difference obtained using the HIOA shown [see Fig. 11(b)] also has two values: $\Delta\varphi \approx 3.267$ rd and $\Delta\varphi \approx 0.135$ rd (with some slight noises added). In both cases, the difference between the two phase difference values is approximately π rd. Meanwhile, the GSA produces a noise-like phase difference [see Fig. 11(a)], indicating its failure of the GSA. Significantly, in the SPP GSA case ($\Delta\varphi \approx 3.866$ rd), only one phase difference value is obtained. This indicates that, although more iterations are needed for SPP GSA to converge, the performance of SPP GSA in the presence of noise is better than either GS/HIOA (1, 39) or HIOA.

In relation to camera quantization [31,32], we note that quantization introduces Gaussian noise [32] (amplitude errors) into the Fourier domain. The result preserved in relation to such noise also indicates the effect of such errors on algorithm performance.

B. ER/HIOA: Single Measurement Phase Retrieval

In all the cases previously discussed, it was assumed that access to the object and Fourier domain amplitude is available. Now, we examine the case when the amplitude in the Fourier domain and some other constraints are available, e.g., the extent or support (i.e., shape) of the object in the space domain. In this case, it is shown that the phase and amplitude in the object domain and the phase in the Fourier domain can be retrieved using the ER/HIOA. In order to retrieve the object given the amplitude of the Fourier image, knowledge of the support of the object image [2–10] (i.e., the set of points over which it is nonzero [33]) must be well known. In other words, locations of the object image's boundary edges must be well known (be sufficiently tight) and sharp (not blurred or slowly tapered) [19].

If support of the autocorrelation of the object (denoted by A) is not a parallelogram, then a tight upper bound on the support of the object image can be estimated or reconstructed by a single-sided locator set found from knowledge of its autocorrelation [33]. The autocorrelation is obtained by taking the inverse Fourier transform of the known intensity in the Fourier domain. If the support of the autocorrelation A is a parallelogram, then the support is called *convex-unambiguous*, which indicates that the support of the object (denoted by S) can be simply reconstructed, since in the 1D case it equals half of the support of the autocorrelation, i.e., $S = A/2$ [33]. In the 2D case, the support of the object can be obtained by taking half of the support of the autocorrelation in each dimension using a scaling operation.

To illustrate how this might work in practice, in our numerical simulation, the classical HIOA is first applied following Eq. (2); then, the ER/HIOA is performed according to Fig. 2. The unusually shaped Lena image shown in Fig. 12(a), acts as the input image with an unknown superimposed spatial phase [shown in Fig. 12(b)] given by $e^{i\theta(m,n)}$, $m, n \in [1, 128]$, where each value of $\theta(m, n)$ is randomly distributed between $-\pi$ and π. As shown in Fig. 12, the Lena image and phase screen information are zero padded to 256 × 256. The resulting amplitude $|\mathcal{F}\{|f(x,y)|e^{i\theta}\}|$ in the Fourier domain is shown in Fig. 12(c).

The second step is to reconstruct the support of the object image. The autocorrelation of the object image is found by

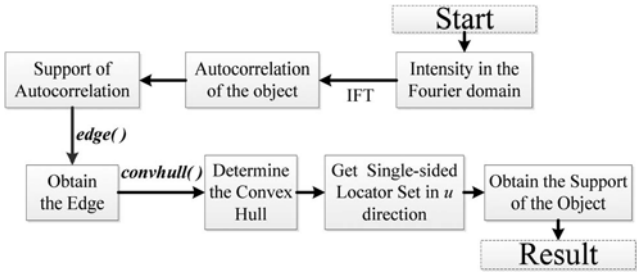

Fig. 13. Process to obtain the tight upper bound on the support of the object (IFT, inverse Fourier transform; *edge*(-) and *convhull*(-) are MATLAB functions [35,36]).

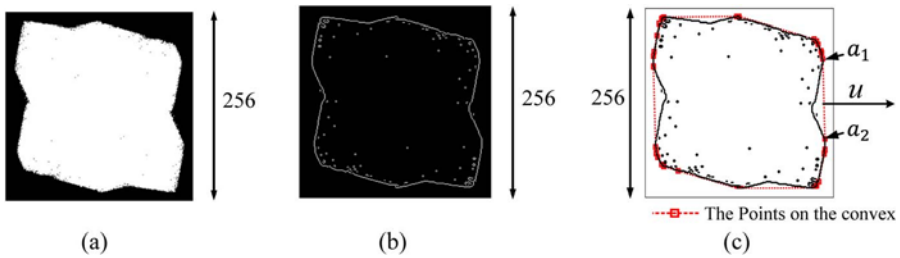

Fig. 14. (a) Support of the autocorrelation of the input object. (b) Edge of the support of the autocorrelation. (c) Convex hull and the maximum points in the, i.e., a_1 and a_2 u direction.

taking the inverse Fourier transform of the intensity of the Fourier image. The support of the autocorrelation of the object image, denoted by A, can be determined from the autocorrelation of the object, which is fairly straightforward. Several steps are then taken to determine the tighter upper bound on the support of the object. First, after obtaining A, we need to obtain the convex hull (the convex hull of a set X is given by the smallest convex subset containing X [33]), before obtaining the single-sided locator set L (a single-sided locator set for A is compact, which contains a translation of S or $-S$ for all supports S that generate A [34]). We note that these complex operations are well described by Fig. 3 in Section 3 of [33]. Because all the points inside A will be considered during the search of the convex hull, in order to decrease the computing load when searching the convex hull of A, we only obtain the pixels on the edge of A and then only search the convex hull between those points. This speeds up the search, since only the points on the edge are considered, and there are much fewer of these than the total number of points inside A. The set of maximal or edge points can be determined, as defined in [34]. This is discussed later in relation to Fig. 14. In this way, tight upper bounds on the support of the object are determined from the maximal points [34]. The process is illustrated in Fig. 13.

For the case discussed in Fig. 12, support of the autocorrelation of the object image, denoted by A, is shown in Fig. 14(a). The edge, shown in Fig. 14(b), is obtained using the built-in MATLAB function "*edge*(-)" [35]. Figure 14(c) shows the resulting convex hull obtained using the MATLAB function "*convhull*(-)" [36]. Points $a_1(x, y)$ and $a_2(x, y)$ on the convex hull of A are the set of maximal points in the u direction (where u denotes the chosen unit vector in this paper), as shown in Fig. 14(c) following [34]. $L = A \cap (A + a_1) \cap (A + a_2)$ is a single-sided locator set for A, which is presented by the white region shown in Fig. 15(a). Other single-sided locator sets [27] are not discussed in this paper. The resulting tighter upper bound on the support of the object obtained from Fig. 15(a) is shown in Fig. 15(b). This operation is discussed in detail in [27]. As shown in Fig. 15(b), the resulting support is not, in fact, the correct support but contains some slight differences from the true support of the object shown in Fig. 12(a). In our simulation, only the two-point rule to determine the single-sided locator set is used. We note that other rules to more accurately determine the single-sided locator set, in order to obtain tighter upper bounds on the support of the object, are discussed in [34].

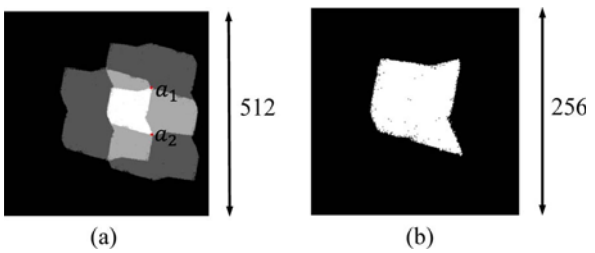

Fig. 15. (a) Determining the support of the object using the single-sided locator set $L = A \cap (A + a_1) \cap (A + a_2)$. (b) Resulting tighter upper bound on the support of the input object.

Given a reasonably tight upper bound on the support of the object image and the amplitude of the Fourier image, the HIO and ER/HIO algorithms can be applied, with $K = 1000$ iterations, to perform single-measurement-based phase retrieval. In all cases, the same conditions are used at the start of the different phase retrieval algorithms, e.g., the same initial guess of the phase in the Fourier plane.

To produce the SSE results shown in Fig. 16, $K_1 = 1$ iteration using ERA followed by 49 iterations using HIOA are performed, i.e., ER/HIOA (1, 49), with a total of $K_p = 50$ iterations in each cycle. The parameter value $\beta = 0.5$ is used in the classical HIOA. The ER/HIOA is performed for 12 cycles followed by 400 ERA iterations.

In Fig. 16, the (a) curve (blue) indicates when just the HIOA is applied, giving an SSE value of ~ -4 dB after 1000 iterations, after which no further improvement is observed. When the ERA alone is applied, a more rapid drop to ~ -16 dB after 1000 iterations is observed [see (b) curve

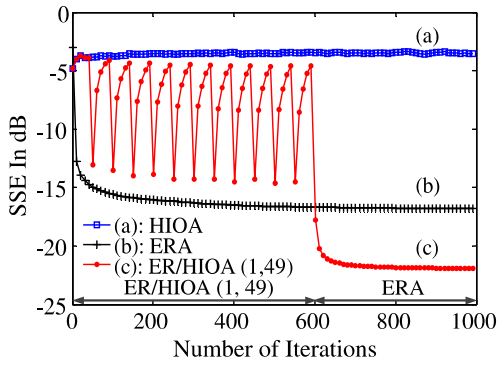

Fig. 16. SSE values using: (a) HIOA, (b) ERA, and (c) ER/HIOA (1, 49) + 400 ERA.

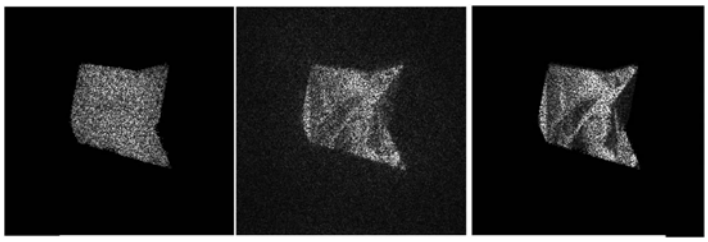

Fig. 17. (a) Resultant retrieved object image ($\overline{\text{MSE}} = 1544.5$) using ERA alone. (b) Resultant retrieved object image ($\overline{\text{MSE}} = 2210.3$) using HIOA. (c) Retrieved object image ($\overline{\text{MSE}} = 1173.7$) using ER/HIOA (1, 49) + ERA (400).

(black)]. Therefore, it seems the performance of the ERA is better than that of the HIOA. However, exactly the opposite behavior is observed when applying the two algorithms for a similar case. The (c) curve (red) shows the SSE value when ER/HIOA (1, 49) is applied for 12 cycles followed by the ERA alone for 400 iterations. It is seen that, after the full 1000 iterations, the ER/HIOA has dropped to ~ – 22 dB.

In order to further quantify the performance of the algorithms, the original and retrieved images are compared using the mean squared error (MSE) as defined by

$$\text{MSE} = \left[\sum_{m=1}^{M}\sum_{n=1}^{N}\{I'(m,n) - I(m,n)\}^2\right][MN]^{-1}, \quad \textbf{(8)}$$

where, in this case, $M \times N = 256 \times 256$ and I' and I represent the retrieved and original images, respectively. Examples of the retrieved images are shown in Fig. 17 (the input is shown in Fig. 12). The algorithms examined in Fig. 16 were each run 10 times with different initially guessed random phases in the Fourier domain. As shown in Fig. 17, the average MSE over the 10 runs is $\overline{\text{MSE}} = 1544.5$ for Fig. 17(a) when the ERA alone is applied, $\overline{\text{MSE}} = 2210.3$ for Fig. 17(b) when HIOA alone is applied, and $\overline{\text{MSE}} = 1173.7$ for Fig. 17(c) when using ER/HIOA (1,49) + ERA (400). Although the MSE value obtained when the HIOA is used is higher than those obtained when using the ERA alone, the Lena image can be visually identified when the HIOA is applied [see Fig. 17(b)], while the ERA retrieved Lena image [Fig. 17(a)] appears to be noise-like. However, it should be noted that the MSE value found when using the HIOA is only higher than that found when using the ERA because the noise appearing in the zero padded area outside Lena image, shown in Fig. 17(b), contributes to the higher MSE value. After removing the noise outside the support [see Fig. 15(b)], the average MSE value inside the support is 1238.3 for Fig. 17(b). We conclude that ER/HIOA works much better than the HIOA alone and results in a higher-fidelity retrieved Lena image with lower image noise.

The phase differences $\Delta\varphi = \text{mod}(\varphi - \varphi'_k, 2\pi)$ in the Fourier domain retrieved using the ER, HIO, and ER/HIO (1, 49) algorithms are presented in Figs. 18(a), 18(b), and 18(c), respectively.

As shown in Fig. 18, the phase difference retrieved using the ERA [Fig. 18(a)] is more noise like compared with either that of the HIO [Fig. 18(b)] or ER/HIOA (1, 49) [Fig. 18(c)]. That means the HIOA and ER/HIOA (1, 49) perform better than the ERA. Carefully examining the phase differences, i.e., Figs. 18(b) and 18(c), we note they are not constant compared to the previous results in Fig. 9, indicating that the performances of the HIOA and ER/HIOA (1, 49) require further improvement. In part, the poorer performance reflects the fact that the tight upper bound on the object found numerically is not the true support of the object. This leads to poor performance by the algorithm.

Examining Fig. 16(c), for the ER/HIOA (1, 49) case, it can be seen that, when the single iteration of ERA is performed, the SSE value repeatedly drops to below –15 dB, while for the following 49 HIOA iterations the SSE value typically increased back up to –5 dB. Does this mean the SSE value will keep dropping if we were to continue to perform more than $K_1 = 1$ ERA iteration and that, as a result, a more visually identified Lena image will be obtained with lower MSE values? We modified the ER/HIOA, changing the number of ERA iterations performed K_1 from 2 to 50 in steps of 2 ($K_1 = 2, 4, \ldots, 50$) for a fixed cycle of length $K_p = 50$ and ran the algorithm applying the same conditions used above, i.e., with the ER/HIOA being performed during the first 12 cycles followed by 400 iterations of the ERA. The algorithm with

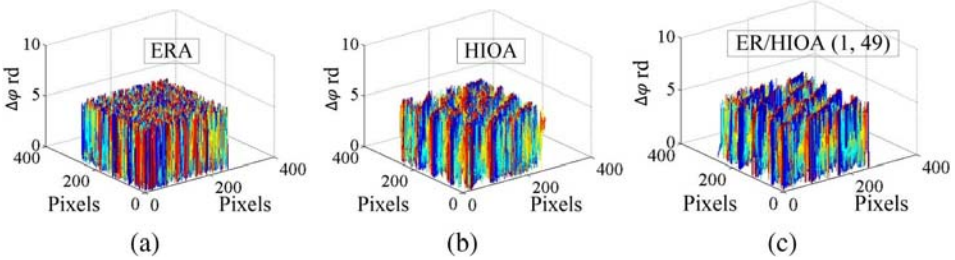

Fig. 18. $\Delta\varphi$ retrieved following 1000 iterations using (a) ER, (b) HIO, and (c) ER/HIO (1, 49) + ERA (400) algorithms.

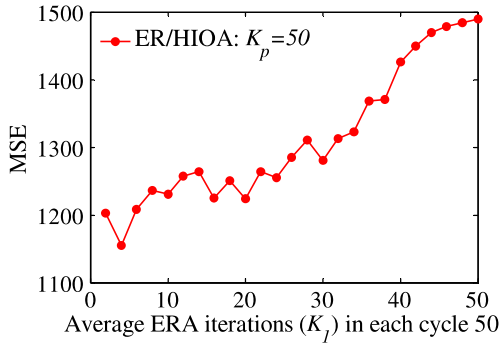

Fig. 19. MSE values between the retrieved and the original Lena images for different K_1 in each cycle using the ER/HIO algorithms: (2, 50) to (50, 0). (12 cycles + ERA (400) 1000 iterations in total.)

different K_1 were each run 10 times with different initially guessed random phases in the Fourier domain. Then the MSE values (between the retrieved and the original Lena images) were used to test performance of the different ER/HIO algorithms. The average MSE over 10 runs between the retrieved and the original Lena images is presented in Fig. 19.

From Fig. 19, we can see that increasing the number of iterations of the ERA in one cycle does not consistently produce lower MSE values. In fact, the SSE values tend to be larger as K_1 increases, although some variations are observed. We recall that, as previously demonstrated in Fig. 16(a), when only the ERA is used (50, 0), the object image in the space domain is not retrieved.

4. CONCLUSION

In this paper, two new phase retrieval algorithms based on two intensity measurements—the spatial phase perturbation Gerchberg–Saxton algorithm and the combined GS hybrid input output algorithm—are introduced. Using numerical simulations, it is shown that superior phase retrieval is provided with significant improvement over the results achieved using either the GSA or HIOA alone. For both modified algorithms, the sum squared error values drop rapidly to acceptable values, successfully retrieving the unknown phases in the space and in Fourier domains. This means that both algorithms can jump out of local minima and converge to the global minimum. Comparisons between the SPP GSA and GS/HIOA are presented. It is shown that the cycle-optimized GS/HIOA converges much faster than the SPP GSA.

In the presence of Gaussian noise, the performance of the SPP GSA is better than either the GS/HIO (1, 39) or HIO algorithms.

In relation to camera quantization [31,32], we note that quantization introduces Gaussian noise [32] (amplitude errors) in the Fourier domain. The result, preserved in relation to such noise, also indicates the effect of such errors on algorithm performance.

Next, the problem of retrieving the object and both phases given only the amplitude in the Fourier domain is addressed. It is shown how, using standard MATLAB functions, tight upper bounds on the support of the object can be determined using a single-sided locator set (denoted by L) in a given direction (denoted by u). Having determined tight upper bounds on the support of the object, both the HIO and the ER/HIO algorithms have been applied to completely retrieve the object information (amplitude and phase) in the space domain. Numerical simulation shows that, using the ER/HIOA, we can retrieve the object with smaller MSE values and lower noise levels compared with the performance of the HIOA alone.

In Part II of this paper, the proposed algorithms are employed to attack amplitude encoding and phase encoding classical double random phase encryption systems. Known plaintext ciphertext attacks and ciphertext-only attacks are discussed.

Irish Research Council for Science, Engineering and Technology (IRCSET); Science Foundation Ireland (SFI).

C. Guo is supported by a University College Dublin China Scholarship Council joint scholarship. S. Liu is supported by School of Medicine, Washington University in St. Louis.

REFERENCES

1. R. W. Gerchberg, "A practical algorithm for the determination of phase from image and diffraction plane pictures," Optik **35**, 237–246 (1972).
2. J. R. Fienup, "Reconstruction of an object from the modulus of its Fourier transform," Opt. Lett. **3**, 27–29 (1978).
3. J. Miao, T. Ishikawa, E. H. Anderson, and K. O. Hodgson, "Phase retrieval of diffraction patterns from noncrystalline samples using the oversampling method," Phys. Rev. B **67**, 174104 (2003).
4. S. Marchesini, H. He, H. N. Chapman, S. P. Hau-Riege, A. Noy, M. R. Howells, U. Weierstall, and J. C. H. Spence, "X-ray image reconstruction from a diffraction pattern alone," Phys. Rev. B **68**, 140101 (2003).
5. H. M. L. Faulkner and J. M. Rodenburg, "Movable aperture lensless transmission microscopy: a novel phase retrieval algorithm," Phys. Rev. Lett. **93**, 023903 (2004).
6. X. Xiao and Q. Shen, "Wave propagation and phase retrieval in Fresnel diffraction by a distorted-object approach," Phys. Rev. B **72**, 033103 (2005).
7. Y. J. Liu, B. Chen, E. R. Li, J. Y. Wang, A. Marcelli, S. W. Wilkins, Y. C. Tian, K. A. Nugent, P. P. Zhu, and Z. Y. Wu, "Phase retrieval in x-ray imaging based on using structured illumination," Phys. Rev. A **78**, 023817 (2008).
8. M. C. Newton, R. Harder, X. Huang, G. Xiong, and I. K. Robinson, "Phase retrieval of diffraction from highly strained crystals," Phys. Rev. B **82**, 165436 (2010).
9. F. Zhang and J. M. Rodenburg, "Phase retrieval based on wave-front relay and modulation," Phys. Rev. B **82**, 121104 (2010).
10. M. C. Newton, "Compressed sensing for phase retrieval," Phys. Rev. E **85**, 056706 (2012).
11. J. Miao, D. Sayre, and H. N. Chapman, "Phase retrieval from the magnitude of the Fourier transforms of nonperiodic objects," J. Opt. Soc. Am. A **15**, 1662–1669 (1998).
12. V. Elser, "Phase retrieval by iterated projections," J. Opt. Soc. Am. A **20**, 40–55 (2003).
13. W. Chen and X. Chen, "Quantitative phase retrieval of a complex-valued object using variable function orders in the fractional Fourier domain," Opt. Express **18**, 13536–13541 (2010).
14. Y. Zhang, G. Pedrini, W. Osten, and H. J. Tiziani, "Whole optical wave field reconstruction from double or multi in-line holograms by phase retrieval algorithm," Opt. Express **11**, 3234–3241 (2003).
15. G. Liu and P. D. Scott, "Phase retrieval and twin-image elimination for in-line Fresnel holograms," J. Opt. Soc. Am. A **4**, 159–165 (1987).
16. G. Situ, J. P. Ryle, U. Gopinathan, and J. T. Sheridan, "Generalized in-line digital holographic technique based on intensity measurements at two different planes," Appl. Opt. **47**, 711–717 (2008).

17. J. R. Fienup, "Phase retrieval algorithms: a comparison," Appl. Opt. **21**, 2758–2769 (1982).
18. J. R. Fienup, "Phase retrieval using boundary conditions," J. Opt. Soc. Am. A **3**, 284–288 (1986).
19. J. R. Fienup, "Reconstruction of a complex-valued object from the modulus of its Fourier transform using a support constraint," J. Opt. Soc. Am. A **4**, 118–123 (1987).
20. J. R. Fienup, "Reconstruction of objects having latent reference points," J. Opt. Soc. Am. **73**, 1421–1426 (1983).
21. E. Osherovich, M. Zibulevsky, and I. Yavneh, "Approximate Fourier phase information in the phase retrieval problem: what it gives and how to use it," J. Opt. Soc. Am. A **28**, 2124–2131 (2011).
22. X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett. **31**, 1044–1046 (2006).
23. X. Peng, H. Tang, and J. Tian, "Ciphertext-only attack on double random phase encoding optical encryption system," Chin. Phys. Soc. **56**, 2629–2636 (2007).
24. http://en.wikipedia.org/wiki/Ciphertext-only_attack.
25. J. R. Fienup and C. C. Wackerman, "Phase-retrieval stagnation problems and solutions," J. Opt. Soc. Am. A **3**, 1897–1907 (1986).
26. A. Fannjiang and W. Liao, "Phase retrieval with random phase illumination," J. Opt. Soc. Am. A **29**, 1847–1859 (2012).
27. M. Köhl, A. A. Minkevich, and T. Baumbach, "Improved success rate and stability for phase retrieval by including randomized over relaxation in the hybrid input output algorithm," Opt. Express **20**, 17093–17106 (2012).
28. S. Hattanda, H. Shioya, Y. Maehara, and K. Gohara, "*K*-means clustering for support construction in diffractive imaging," J. Opt. Soc. Am. A **31**, 470–474 (2014).
29. U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, "A known-plaintext heuristic attack on the Fourier plane encryption algorithm," Opt. Express **14**, 3181–3186 (2006).
30. MathWorks, http://uk.mathworks.com/help/matlab/ref/mod.html.
31. C. Guo, S. Liu, and J. T. Sheridan, "Optical double image encryption employing a pseudo image technique in the Fourier domain," Opt. Commun. **321**, 61–72 (2014).
32. S. Liu, B. M. Hennelly, and J. T. Sheridan, "Digital image watermarking spread-space spread-spectrum technique based on double random phase encoding," Opt. Commun. **300**, 162–177 (2013).
33. J. R. Fienup, T. R. Crimmins, and W. Holsztynski, "Reconstruction of the support of an object from the support of its autocorrelation," J. Opt. Soc. Am. A **72**, 610–624 (1982).
34. T. R. Crimmins, J. R. Fienup, and B. J. Thelen, "Improved bounds on object support from autocorrelation support and application to phase retrieval," Opt. Soc. Am. A **7**, 3–13 (1990).
35. MathWorks, http://www.mathworks.co.uk/help/images/ref/edge.html.
36. MathWorks, http://www.mathworks.co.uk/help/matlab/ref/convhull.html.